UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. DENY MITROVICH	No. 18 CR 789 Judge Gary Feinerman

GOVERNMENT'S SURREPLY TO DEFENDANT'S MOTION TO COMPEL

The UNITED STATES OF AMERICA, by JOHN R. LAUSCH, JR., United States Attorney for the Northern District of Illinois, respectfully submits this surreply to defendant's motion to compel. For the following reasons, the motion should be denied.

I. PROCEDURAL BACKGROUND

Defendant has moved the court to compel production of the following discovery:

> 4. Any and all discovery relating to the FBI and MCCU['s] "ability to identify IP addressed associated with certain users of TorChat and certain hidden services" as referenced on MITRO_00001.[1] This includes but [is] not limited to the name of the software used, any and all manuals related to the software, logs kept throughout [the] course of [the] investigation, all training materials, including but not limited to training records, certification records, training standards, and training manuals, all policies and procedures regarding use of this software, names and curriculum vitae of any and all individuals who operated, and any and all records utilized by FBI and MCCU during course of this investigation as it relates to this software; and,
>
> 5. Any and all communications between the FBI/MCCU and QPS and DIA throughout Operation Downfall II, as referenced on MITRO_00001-

[1] Defendant clarified that this request also applied to, "the software used to redirect users from the 'Tor' network to the open Internet."

> 00002, including email communications, letters, and any and all attachments including the reports generated of each user through TLZ sting that were "generated by QPS/DIA and provided to the MCCU for further identification."

Dkt. No. 48 at 4-5.[2]

In his original motion, defendant claimed these requested items were material to his defense because: (1) he had a reasonable expectation of privacy in his IP address since he "took additional steps [to] keep his IP address private and secret by using the 'Tor' network on the 'dark web'" (*id*. at 11); and (2) the requested communications between the FBI and foreign agencies would allow defendant to "establish that the FBI and QPS/DIA were working in concert with one another at the time the IP address was seized" (*id*. at 9).

The government's response to this motion established that defendant's legal basis for requesting these materials was meritless, because he voluntarily clicked the link that caused him to leave Tor, and he had no reasonable expectation of privacy in his IP address (despite his use of Tor). Dkt. No. 53. The government further distinguished this case from those cases involving the so-called "Network Investigative Technique" (NIT) "in which the target computers were essentially taken

[2] As set forth above, Request 5 asks, in part, for "the reports generated of each user through TLZ sting that were 'generated by QPS/DIA and provided to the MCCU for further identification.'" This part of Request 5 was identical to Request 3, which was already made available to defendant.

over and compelled to transmit identifying information to government computers." *Id.* at 5-6.[3]

In his reply brief, defendant tried to bridge the gap between this case and the NIT cases by asserting for the first time that—in this case—for defendant to have been redirected outside of Tor, "a malicious code (or 'malware') had to be installed on his computer." Dkt. No. 56 at 1. ("Essentially, because of the way the Tor Network and Tor Browser operates, the hyperlink must have contained malware that forced Mr. Mitrovich's computer to send the identifying information to QPS/DIA or forced it to exit from the Tor Browser and onto the open internet. It would have been impossible to do so otherwise."). Defendant supported this factual claim by referencing internet news articles and a present-day Tor FAQ (as opposed to Tor materials dating to 2014).

Defendant's legal argument shifted along with his facts: "Even though one may not have had a reasonable expectation of privacy in some of the information on the computer, the courts held that a person does have a broader expectation in the computer itself through, at least in part, the Fourth Amendment property-based approach." *Id.* at 2.

[3] The government's brief continued: "Here, by contrast, QPS/DIA merely planted a hyperlink that—when voluntarily clicked by defendant—loaded a video file that was not within the Tor network. Defendant's computer was not compelled to do anything other than what defendant asked it to do when he voluntarily clicked the link and viewed the video." *Id.*

II. QPS/DIA DID NOT DOWNLOAD MALWARE INTO DEFENDANT'S COMPUTER OR OTHERWISE INVADE HIS COMPUTER SO AS TO IMPLICATE THE FOURTH AMENDMENT

As a factual matter, and contrary to defendant's assertions, the technique used to obtain defendant's public IP address did not involve downloading malware onto his computer or otherwise invading the property of his computer. Nor did simply using Tor at that time make this technique impossible absent malware.

The prosecution team in this case recently interviewed FBI Supervisory Special Agent Brooke Donahue. According to a report of that interview (attached as Exhibit A), Donahue has been a supervisor in the FBI's Child Exploitation Operations Unit (CEOU) for ten years.[4] The CEOU was the unit responsible for investigating "The Love Zone" website, and Donahue was personally involved in the case.

Although he does not know the "minute details" of the technique used by QPS/DIA to uncover defendant's public IP address, Donahue is familiar with what the technique entailed—as well as what it did not entail. Donahue's knowledge is based on communications he had with Australian/New Zealand law enforcement personnel.

According to Donahue, after the Australians took control of the TLZ server and placed it back online in Australia, the Australians posted a video link to TLZ. When users of TLZ clicked on the link, it advised them it would be taking them outside of

[4] The CEOU was formerly called the MCCU.

Tor. Once they were outside of Tor on the clear web, the video would play and the user's IP address was captured.

Contrary to defendant's assertions in his reply brief, Donahue confirmed that QPS/DIA's technique did not involve hacking, using/inserting malware, or using escalated privileges on a user's computer. More broadly, there was no information collected from inside the user's computers. In order for this technique to work, it took the actions of the subject, who clicked on the link. Again, contrary to defense counsel's claims about the nature of Tor, Donahue confirmed that the mere use of Tor did not preclude this technique from working.

* * *

Donahue's account makes clear that defendant's revised, property-based theory for application of the Fourth Amendment is unfounded. Instead, as argued in the government's response brief, defendant's motion to compel should be denied because (1) defendant voluntarily clicked the link that placed him outside of Tor, and (2) defendant did not have a reasonable expectation of privacy in his IP address.

To the extent defendant persists in a contrary view of the facts (despite the evidentiary record described above), he should be made to offer some relevant and particularized evidence (e.g., an expert report) in order to meet his burden.

III. THERE IS NO FACTUAL BASIS TO BELIEVE THE FOURTH AMENDMENT APPLIED TO THE CONDUCT OF QPS/DIA

Defendant's discovery motion should also be denied because there is no basis to believe the Fourth Amendment applied to the alleged "search" conducted by the foreign law enforcement agencies—QPS and DIA—on defendant's public IP address.

In this case, the exclusionary remedy defendant seeks is available only if, among other things, the alleged "search" was the result of a "joint venture" between the FBI and the Australian and New Zealand agencies. The legal standard for finding a "joint venture" was comprehensively stated by the district court in *United States v. Agosto-Pacheco*:

> One exception to the general inapplicability of the Fourth Amendment exclusionary rule to foreign authorities' searches occurs "where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." [*United States v. Valdivia*, 680 F.3d 33, 51–52 (1st Cir. 2012)]. This exception is known as the joint venture doctrine. *Id*. . . . Ascertaining whether the joint venture doctrine is satisfied presents a "factually based issue" that involves "applying a legal label to a complex set of facts." [*United States v. Hensel*, 699 F.2d 18, 25 (1st Cir. 1983)]. Pursuant to the doctrine, courts examine the nature and extent of cooperation among, and the activities of, United States and foreign authorities. *See id*. One court identified the following four-factor test for evaluating the issue: (1) whether American authorities initiated the investigation in the foreign country; (2) whether American authorities were involved in the decision to seek the foreign wiretap; (3) whether American agents controlled, directed, or supervised the foreign wiretap; and (4) whether American agents participated in "the implementation of the wiretaps and recording of conversations." *United States v. Marte*, Criminal No. 16-30044, 2018 WL 4571657, at *6 (D. Mass. Sep. 24, 2018) (quoting *Valdivia*, 680 F.3d at 52). Courts also look to the relative interest of the United States and foreign governments in the matters under investigation. Wayne R. LaFave, 1 Search & Seizure § 1.8(h), at 456 (5th ed. 2012) (hereinafter LaFave).

> Some courts have found the facts before them to satisfy the joint venture doctrine. In *Peterson*, [812 F.2d 486, 490 (9th Cir. 1987)], the court found a joint venture where United States authorities characterized their actions as a "joint investigation" and were "involved daily in translating and decoding intercepted transmissions, as well as advising [foreign] authorities of their relevance." In *Powell v. Zuckert*, 366 F.2d 634, 639–40 (D.C. Cir. 1966), the court held that the Fourth Amendment applied to a search by United States and Japanese officials where the only Japanese interest served was compliance with a treaty obligation.
>
> But the majority of cases find no joint venture. *United States v. Morrow*, 537 F.2d 120, 140 (5th Cir. 1976*); see also* LaFave, 1 Search & Seizure § 1.8(h), at 452 n.301 (collecting cases). For example, in *Valdivia*, 680 F.3d at 52, there was no sufficient basis to find a joint venture where foreign authorities initiated an investigation; a wiretap was not requested, organized, or monitored by United States authorities; and United States authorities only received recorded conversations after the investigation concluded. In *United States v. Behety*, 32 F.3d 503, 511 (11th Cir. 1994), the court found no joint venture where United States authorities relayed information facilitating a search, were present at the search, and videotaped part of it. In *United States v. LaChapelle*, 869 F.2d 488, 490 (9th Cir. 1989), testimony from a Canadian official that there was no United States involvement in initiating or controlling a wiretap was a sufficient basis on which to defeat claims of a joint venture.

2019 WL 4566956, *3–6 (D. Puerto Rico Sept. 20, 2019).

Here, the facts offered by SSA Donahue demonstrate there was no joint venture between the FBI and QPS/DIA.

More specifically, according to Donahue, the FBI did not provide any information to, or make requests of, Australia or New Zealand. Instead, the FBI provided investigative leads to the Dutch after learning TLZ was located in the Netherlands. The FBI did not direct the Dutch authorities in connection with this lead.

Donahue explained that the FBI and other governmental law enforcement agencies share information regarding child exploitation investigations because it is a crime that crosses borders and requires international cooperation. Information regarding the investigation was being shared verbally between the FBI and Dutch authorities. The Dutch authorities later notified the FBI that the IP addresses for the administrators of TLZ came back to Australia. At that point in the investigation into TLZ, it was an operation between the Dutch, Australian, and New Zealand authorities. The FBI was not a part of this investigation.

Australia worked with the Dutch authorities to get a copy of the server for TLZ. The Australian authorities were then able to put the server back online in Australia. It was at this point that QPS/DIA began using the investigative technique in question to identify the public IP addresses of TLZ users. The Australian authorities used this technique without advice from the FBI, or advance notice to the FBI. The Australian authorities informed the FBI of their use of this technique after the fact.[5] The Australian authorities advised other governmental law enforcement agencies—including the FBI—for deconfliction purposes.

One of the TLZ users who the Australian authorities identified through this technique was "Cyberguy." The Australian authorities determined "Cyberguy" was located in the United States, and they passed this information on to the FBI. Once it

[5] In a separate email to the author of the attached report, SSA Donahue explained that, "The FBI was informed of the Australian operation after they had already taken control of TLZ and were prepared to utilize their technique to identify individual users."

was determined where "Cyberguy" was specifically located, the information was forwarded to FBI Chicago.

Besides sending the initial information to the Dutch authorities regarding TLZ's hosting location, and verbally communicating with both the Dutch and Australian authorities throughout the investigation, the FBI only received lead packets for users of TLZ who were identified as residing in the United States. The FBI did not have access to the foreign authorities' investigative files, and vice versa. The FBI did not advise other governmental law enforcement agencies on what to investigate. It was an arm's length relationship between the FBI and foreign law enforcement authorities that involved deconfliction and lead sharing.

* * *

In summary, the international information sharing and deconfliction involved in this case did not render FBI-CEOU a "participant" in the QPS/DIA operation, or make investigators with QPS/DIA agents of the United States. As such, defendant's exclusionary theory also lacks merit for this reason as well. And discovery on the topic of the "search" of his IP address by QPS/DIA—including communications with the FBI—would therefore not be material to his defense.

III. CONCLUSION

For the foregoing reasons, the government respectfully requests that the court deny defendant's motion to compel.

Dated: March 16, 2020

Respectfully Submitted,

JOHN R. LAUSCH, JR.
United States Attorney

By: /s/ *Andrew C. Erskine*

Andrew C. Erskine
Assistant United States Attorney
219 S. Dearborn St., Room 500
Chicago, Illinois 60604
(312) 353-1875